The Information Commissioner's response to the Department for Business, Energy & Industrial Strategy's consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities

Introduction

The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation ('GDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Commissioner welcomes the opportunity to respond to the Department for Business, Energy & Industrial Strategy's (BEIS) consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities. The Commissioner's response to this consultation relates to those sections which raise information rights considerations.

The Commissioner acknowledges the objectives of the proposed reforms of the Companies House register which include improving transparency and accountability, increasing accuracy and reducing economic crime. The consultation contains some measures which will introduce new protections for personal data held on the register; such measures are welcome. Equally, the consultation includes proposal for new processing of personal data, including categories of sensitive personal data. Such processing must be introduced in compliance with data protection legislation and with appropriate risk assessments and safeguards in place. We welcome the open approach to engagement with the ICO that Companies House and BEIS have adopted to date.

Data Protection Impact Assessments

As the proposed measures would involve large scale processing and the potential collection of biometric data by Companies House, we would highlight the requirements under GDPR to conduct a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to the rights and

freedoms of individuals. This includes specified types of processing such as the systematic and extensive evaluation of individuals' personal aspects and large scale processing of sensitive personal data.

In addition, the ICO's published guidance on DPIAs specifies further processing types for which an assessment must be carried out, including the use of new technologies, profiling individuals on a large scale, matching or combining datasets from different sources, and collecting data from sources other than the data subject without providing them with fair processing information.

DPIAs act as key tool in helping to ensure that personal data can be used in innovative ways without infringing upon the fundamental privacy rights of individuals. It should also be noted that the ICO must be consulted in cases where a DPIA identifies a high risk and measures cannot be taken to reduce this risk. A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Identity verification

The proposals for verification of identity will necessitate the large-scale processing of personal data. Consideration must therefore be given to how that processing can be performed in a manner compliant with data protection obligations.

The responsibilities of organisations processing personal data are described in the General Data Protection Regulation (GDPR). The GDPR also lays out the rights of data subjects. Consideration of how to satisfy these rights will need to be in scope of the identity verification process. If an exemption to these rights requests is to be applied under a Data Protection Act schedule, this would need to be justified and documented.

Biometric data processing

Article 9 of the GDPR describes special categories of personal data. Processing biometric data for the purpose of identifying an individual falls into this category. When processing special category data, in addition to the lawful bases required

for processing personal data, one of the additional conditions described in Article 9(2) would also be required to be met.

Data controllers should assess the necessity and proportionality of such processing, and we would expect to see consideration of whether the same objective can be achieved through less intrusive means.

If biometric data processing forms part of the proposed identity verification process, then consideration should be given to the greater protections afforded to special category data the organisational and technical means necessary to process it safely and securely.

Processing of identity verification data by third parties

The consultation asks (in Q4): "Do you agree that the preferred option should be to verify identities digitally, using a leading technological solution?" Any proposed solution would need to allow compliance with data protection law and principles.

In the event that a third party processes the data on behalf of Companies House, this would need to be done in a manner compliant with the responsibilities of the controller and processor as described in Chapter 4 (articles 24-43) of the GDPR.

Gender reassignment

Q29 relates to the replacement of a name on the register following a gender reassignment. The data protection principles outlined in GDPR article 5 address the fairness and accuracy of processing and of keeping records up to date. Where an individual informs a processor of a change to their personal data (including their chosen name) it is appropriate that the processing of that data is updated accordingly.

Public and non-public information

We welcome the proposal to maintain differentiation between data publicly displayed in the register and that which can be accessed by Companies House staff. This is in line with the requirement under article 5 of the GDPR to process data in a manner which is necessary for the purposes for which they have been collected and to prevent unauthorised processing.

Data sharing

We note that a number of references are made within the consultation to sharing appropriate information with relevant partners, such as the police and other law enforcement authorities. Controllers need to be aware of their obligations to data protection law in terms of data sharing: respective responsibilities and lawful basis must be clear, and data that is shared must be necessary and relevant. The Commissioner supports the appropriate use of data sharing to enable better regulation of the information contained in the Companies House register. The DPA and GDPR should not be seen as a barrier to data sharing which is justified and proportionate.

Ensuring that appropriate procedures are in place - such as data sharing agreements where appropriate - will help to build the necessary relationships with partners to enable the right information to be shared as quickly as possible, whilst meeting data protection obligations. The ICO is currently in the process of updating its data sharing code of practice. The draft code for consultation has been published here: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/.

Machine learning

The use of machine learning to create a ”risk engine” to process and identify information which may be fraudulent or incorrect should take into account Article 22 of the GDPR which describes the rights of the individual regarding automated individual decision-making, including profiling.

Further comments

Finally, the Commissioner would welcome further engagement regarding the issues covered in this consultation. She is supportive of initiatives that allow personal data to be used in ways that benefit individuals while also fulfilling her commitment to increase consumer trust in the processing of personal data.

In particular, the Commissioner would like to take this opportunity to highlight the requirements of Article 36(4) of the GDPR, which requires relevant public bodies to consult with the ICO during the preparation for a proposal of a legislative or regulatory measure. Guidance on this obligation may be found here: https://www.gov.uk/government/publications/guidance-on-the-application-of-article-364-of-the-general-data-protection-regulation-gdpr